UNCLASSIFIED

OHNR: OH-2013-86
TRSID: rkkunde//ragenti
QCSID: dpcoole

DOI: Summer 1966
DTR: 19 November 2013
Text Review: 23 Jan 2014
Text w/Tape:

INAME: CALLIMAHOS, Lambros D.
IPLACE: NSA, Fort Meade, Maryland
IVIEWER: Unidentified Moderator

Moderator: This lecture is part of the 1966 Summer Institute for Mathematics and...Mathematicians and Linguists. These people are not the only ones who are here this summer. But these are, for the most part, people who have come to NSA for the first summer and are either juniors or have just graduated. Some of them are graduate students. Some of them have their master's degree. Other interested persons have been invited so that we won't let any of this cryptologic knowledge go to waste. I expect that this gathering this morning reminds Cal((limahos)) of his days back in the '30s when he used to pack them in with his flute. ((Audience chuckles.))

To get back to the Summer Institute, we have 24 mathematicians, 17 linguists from 24 different colleges and universities. We have four from Harvard; one from Maryland; three from Michigan State; four from Middlebury; one from Hampton Institute; two from Wisconsin and two from Vermont; one from Michigan Tech; four from Mary Washington; two from Yale; one from Southern California; one from Cal Tech; one from Brown; one from MIT; one from Mount Holyoke; one from Lehigh; one from Georgetown, two from Indiana; one from Arizona—and you will notice the Dr. Sinkov influence there; one from Pennsylvania; one from Eastern Illinois; one from Iowa; two from Connecticut; and one from Smith. Did I miss any school? Perhaps some of you may wish to come down and chat with someone from your old school after the lecture.

Will those in the Summer Institute please stand so we can see where you are? Only...((Audience applauds.)) The fact that we have standing room only sort of spoils my next remark. I was going to say that only those who stood up will be responsible for the lecture. ((Audience chuckles.))

Mr. Callimahos began his cryptologic career in 1941, when he volunteered for the Signal Intelligence Service in the U.S. Army. He was born in Cairo. And as I said, in the 1930's, he was one of the world's greatest flautists ((a

version of the word "flutist."). As most of you know, he still "flautes". ((Audience laughs.)) He studied at the Julliard School of Music. At 26, he was the youngest professor at the Mozarteum Academy in Salzburg, Austria. And it just now occurs to me that somehow our M ((Group)) recruiter seems to have missed the Mozarteum again this year. ((Audience chuckles.))

Cal is a tea fancier and a snuff sniffer. ((More laughter heard.)) He has a collection of 141 different kinds of snuff. He is a gourmet, a member of the Anteaters Club of Washington. He's the co-author with William Friedman of *Military Crypt I* and *II ((MILCRYPT I and II))*. He wrote the article on codes and ciphers in *Colliers Encyclopedia*. And since he has his alarm set for exactly one hour, I don't want to take any more time away from Cal. Mr. Callimahos. ((Audience applauds.)) ((TR NOTE: Speaking can be heard faintly in the background:)) (B% Did you want to, Bill? Want to speak? Want to, Bill? Just...) (3-4G). ((Audience laughs.))

Callimahos: Fifty-five minutes. ((He pauses.)) This is a strange world we live in. Every year ,the print in the telephone directory seems to be getting smaller and smaller. And every year the NSA summer hirers seem to be getting younger and younger. Ah...Are you (B% awaking)? ((Audience laughs.))

Well, (2-3G) one end of the spectrum, we have Miss (B% Lorraine Dunn)—please stand up—who's recently out of the "mud pie" stage. ((More laughter heard.)) A hand! Come on, gentlemen. ((He begins to applaud, leading the audience into applause.)) And at the other end of the spectrum, we have Dr. Fairbanks. Stand up, Sidney. ((Laughter and applause heard.)) That's alright. Don't overdo it. ((More laughter heard.)) I once thought that Dr. Fairbanks was secretary to Andrew Jackson, but he wasn't. It was Johnson—Ambassador Johnson.

((He clears his throat.)) This is a merger of several lectures, one of which was entitled *26! or Bust*. ((Spoken as "Factorial 26 or Bust.")) ((Audience laughs.)) Thank you. ((Sounds made as if he is using chalk to write on a chalkboard.)) And this number, we'll come to later, to one significant digit. For those who use a slide rule, it is four times 10 to the 26^{th}.

Everybody get it? And for those who like the full number, we have this. ((Sounds of writing on a chalkboard continue.)) However, Dr. (1-2G) points out this is a fallacy indeed because we mustn't preserve the identity. We come to this later. So it really should ((more writing heard.)) However, for all practical purposes, it's the first thing I wrote. ((Laughter heard.))

Cryptology is an ancient profession; in fact, the second oldest profession. ((Audience laughs.)) One that abounds in fascination, and one that has a profound effect on history. In my lecture today. I shall include some lesser known facts of cryptologic history— lifting the curtain more or less discreetly—mostly less—to peek at some of the *dramatls personae* who

made us what we are today: brilliant, dull, humble, bombastic, dedicated, and concerned gentlemen, office politicians. ((Audience chuckles.)) I shall also prove to you that, counter to opinions held by a few of our employees, cryptologists are quite human. Now, sit back and relax, enjoy it. You may not drink or smoke. But those of you who use snuff, may feel free. ((Laughter heard.))

We have to start with communication. And, of course, we have to start with my forbearers—at least I have to. That the ancient Greeks had couriers of course—messengers. And one dodge—this is part of communication—was to shave the head of a slave and inscribe on the bare skin the message. Then you wait a while—deferred message. ((Audience laughs.)) And when the hair grows back, the slave is dispatched—that is, sent to the distant commander at the other end. Not of the slave; I mean of the (3-4B by laughter)). The commander shaves the head of the slave, reads the message, and is aware of the contents. In case it's particularly sensitive correspondence, it's a one-time slave. ((Laughter.)) No. ((Laughter continues.))

The Greeks also used secret inks— juices of berries and whatnot, sputum and other body fluids. The last time I gave this lecture, I said "organic effluvia." That didn't go over, so…

On concealment, which is part of cryptology perhaps, Hieronymous mentions the dodge of putting a message inside the belly of a (B% unskinned) hare. Or covering a tablet with wax. Or messages inscribed, quote, "on leaves covering the putrid ulcers of a disguised beggar." That's owing to Aeneas—not the beggar—the quote.

One interesting thing…This is part of cryptology (B% really). In the British-Indian Wars of around…circa 1840, a message was sent by Lord (B% Ellen) ((writing on chalkboard heard)): "Peccavi"—which in Latin, as you all know, is "I have sinned." However, what he meant was, "I have S-I-N-D-H." In the same war, we have "vovi", which again, as you all know, means "I have owed." ((However, what was meant:)) "I have the city of Oudh."

Now, let me give you some…I'll have to drop facts and figures—that is names and dates. And it won't be for long—for 55 minutes. So bear with me. Early cryptography started with Egyptians really around 1900 B.C. And it's interesting to note that it's priests, ruffians and scoundrels who caused the greatest advance in our science. Thank you. ((Audience chuckles.))

The ancient Hebrews indulged in a form of cryptography. In fact, in Jeremiah 25:26 and also Jeremiah 41:51, as you all know, there are

references to reverse standard writing.

What you may not know is that the Kama Sutra...Now, some of you may not have read this because it's the Hindu art of love. And if you read it too early, you wouldn't have your clearance. ((Audience laughs.)) There are 64 (B% arts) to be practiced by ladies of all stations and is...It is heartwarming to know that the 45th art, amongst many other different types of arts, is that of cryptography. So there! ((Chuckling heard.))

Now we come to 400 B.C. Lysander mentions...Actually, it's Plutarch who mentioned the use by the Greeks of the "scytale"—a marshal's baton, tapered—around which you put the belt, (B% closed) pants. And the message is inscribed in Greek, of course, across the baton. The tape is unrolled. Sent to the distant commander, who has a similar baton. It's put back on, and the message comes out. This is our first transposition system.

The one chapter in the work on fortifications by Aeneas the Tactician had to do with cryptography. This is the first treatise on cryptography. He gave 20 systems for secret correspondence.

100 B.C. Julius Caesar, in corresponding with his buddies Opius, Cornelius, Baudus—I don't know who they were; but anyway they have (B% two) names—used a direct (B% set of alphabets). Set A plain as D cipher. This was too complicated for Augustus, who used the setting A plain is B cipher. It's a lot easier. ((Audience laughs.))

Now, we jump very rapidly to the Papal States, 1200 ((A.D.)). We have...In this era, we have the first systematic crypto correspondence. They had vowel substitution. The consonants were left unchanged—(B% were subject of vowels); and code symbols. Am I speaking too rapidly? Thank you, Jack (B% Spurley). Are you the only one who thinks so? ((Audience laughs.))\

In 1378, Gabriel de Lavinde of Parma, who worked for Clement the VII...In case you doubt the date, it's the other Clement the VII—the anti-pope. Ah...((Lavinde)) Wrote an SOI: signal operating instructions. The manual is in the Vatican. He has a set of keys for 24 (B% correspondence). He used symbols for letters. And he used nulls and several two-letter code equivalents—words and names.

In 1412, Qalqashandi, a Persian living in Egypt, wrote a 14-volume encyclopedia. And in this encyclopedia was the first treatment of both substitution and transposition. And we have in this encyclopedia the first cipher to provide more than one equivalent for a plaintext letter. That's 1412.

In 1470, Leon Battista Alberti of Rome wrote *Trattati In Cifris.* He was an architect, a painter, a musician, a writer on art, a horseman, an athlete.

He was born in 1404 a bastard. A nice guy; but, you know, he was a...((Audience laughs.))...Of a wealthy Florentine family. He went to Bologna U. ((Audience laughs.)) He was the most universal genius of the First Renaissance. He invented the cipher disc and also he conceived a...in this disc, a 336-group enciphered code system.

In 1531—all this on cryptography now—Johannes Trithemius wrote volumes I and II of a projected set of four. His *Polygraphiae* was the first printed book on cryptology. In *Steganographia*–it was the second volume—he continued. He was a magician. Actually, in our business, everything helps. ((Chuckling heard.)) He also classified witches into four categories. We do nowadays into two categories: young and old. ((Audience laughs.)) And he was accused of being in league with the devil. His books were burned. Thank God he wasn't. And, by the way, he is the author/the inventor of the progressive (B% alphabet) system and thought up the gimmick of the square tables.

Now, the meaning of 26! ((spoken as "26 factorial"))—this system here. Ah, God bless you. There are 26! ways of making a simple substitution alphabet using 26 letters. If you have a sequence of symbols for the plain A to Z, under the first letter A, you could put any one of the 26. And you have 25 left for the second, and 24 left for the third, etcetera. Now, this...A big number might lead one to believe that you couldn't possibly solve a simple substitution because, my gosh, you have to make all those trials. Actually, you don't because the probability is .5 that you'd get a result before half that number is reached. ((Laughter heard.))

To understand what this number is, if we had one thousand machines capable of testing one million alphabets per second, it'll take over one billion years to go through the gamut. However, as I said before, you expect a solution in five hundred thou...or five hundred million. The age of the earth is 4.5 billion years, and that of age of man is a hundred thousand years, as Dr. Fairbanks can attest. ((Audience laughs.))

We do solve simple substitution on the base of frequencies because after all you don't have a population that is equally probable. E and T are used much more frequently than (1G), Q, X, Z, which account for only 1.4 percent in English plaintext. Not E and T; the last group I mentioned. And we rely on repetitions and (B% idiomorph) patterns. An A-B-B-A pattern like the word "attack" or "battalion" gives itself away perhaps with...if you consider also the frequencies.

I'll have to skim over some of this because this is a lecture that's from 30 minutes to four hours, depending upon the rate of speech, the condition of

the equipment, and the condition of the audience. ((Audience chuckles.)) However, this is... I say, at 9:30 we can all go back to work. I shudder to think what this is costing the Government. ((Audience chuckles again.))

Now, the first significant departure really from simple substitution was in the use of variants and the use of systems that equalized the frequencies. In other words, if you had a 10 x 10 matrix into which you put 13 E's and nine T's, etcetera, if used adroitly, you could flatten out the frequencies pretty doggone flat.

The first significant breakthrough was really in the latter part of the last century by Sir Charles Wheatstone—and we'll come to him later—who invented the Playfair cipher. This was a cipher in which instead of enciphering letter by letter, you enciphered digraph by digraph: two letters at a time, thus suppressing the frequencies of individual components of these digraphs.

In 1914, Lieutenant... First Lieutenant Mauborgne, who later became Major General, Chief Signal Officer—so you *can* get ahead in this business ((chuckling heard))—wrote *An Advanced Problem in Cryptography and Its Solution*. This is on the Playfair cipher. It's published at Fort Leavenworth. He was going to school. ((Laughter heard.))

In 1902, a chap by the name of Felix or François de la Stelle published for the first time a monome/dinome cipher in which some letters were encrypted by single digits—others by pairs of digits. This is in *Traité de Cryptographie*. However, I found just recently that (B% Matteo Algenti), who flourished about 1560, (B% incorporated) the same thing in a written work. ((He coughs.))

You all know what transpositions are. You retain the same plaintext elements, but shuffle their places. Writing a message backward would be the simplest kind of a transposition system. From these simple ideas of simple substitution and simple transposition, we go to polyalphabetic substitution... ((enunciates more slowly:)) polyalphabetic substitution.

In 1470, Alberti was actually the father of (B% polyalphabeticity). In 1563, Giovanni Battista de la Porta—known to his buddies as (B% "Jyam") Battista de la Porta ((audience chuckles))—born 1535. He was a physicist and a physician. Inventor of the *camera obscura*—predecessor of the Kodak ((audience chuckles)).

He wrote *De Furtiva Literarum Notis*. He had some very racy plaintext examples. I'm sorry I can't give them here. (B% They're) still... I mean... In fact, shocking. ((Audience laughs.)) See me later. ((More laughter heard.))

He is actually the conceiver... Poor choice of word. But he is the inventor of the probable word method, and also the inventor of the first digraphic (B% sector). In his book, he had movable cipher disks right in the dog-gone book. And he portrayed square tables. And he had the first synoptic tables for cipher analysis. We're much concerned with diagnosis

nowadays.

In 1585, Blaise de Vigenère…Not a nobleman. He's from the…this territory of Vigenère. Born 1523. Wrote the *Traicté de Chiffres*. He invented plaintext autokey, and then went to (B% periodic) substitution. He did not invent the Vigenère Table, to which his name is commonly attributed. In his travels in Italy, one of the things he picked up—alright, skip it—was the idea of the square table.

In 1757, we have a remarkable person, a cryptologist whose…Well, I'll give you his name first: Jac((opo)) "Casanova" de Seingalt. He was a cryptologist. He was versed in medicine, mathematics, music, as well as practical anatomy and the lively arts. ((Audience laughs.))

He was a…I got to play this straight. He had an acquaintance. Well, actually more than acquaintance. But he…Miss…Madame d'Urfe was a mystic. And she told him, in one of their cuddlier moments, that she had confided her thoughts to a manuscript through a secret cipher. And he said, "I can read that?" And she said, "No, no you can't." He said, "Oh, yes, I can." Now, she knew he was a great man, but she doubted his ability in this field. ((Audience chuckles.))

And five to six weeks later, he came back and told her that he had solved the cryptogram. And the keyword…This is periodic polyalphabetic substitution. And the keyword was one belonging to no language. Well, she was shocked. Actually, the keyword was "Nabucodonosor"—which is the Italian equivalent, as you all know, of "Nebuchadnezzar". And this is a quote from "Jackie:" "That day, I became master of her soul and I abused my power." I'm not sure what that means. ((Laughter heard.)) I'm just passing it on for your…((More laughter heard.))

What startled me was that Casanova solved a periodic polyalphabetic substitution one hundred years before the method of solution was published in open domain. And I thought that…He was a great discoverer. I thought that—great scholar also—that he had discovered this in his…the few leisure moments he had.

But Mr. Friedman points out that Casanova, having been in court circles and he was…He knew the ins and outs in many fields. He…Casanova could well have been in a "black chamber." And I mean this in the cryptologic sense of the word, thank you. ((Audience laughs.)) And was privy to the s…That's a poor word. Was ((audience laughs again))…Well, he knew these secrets that didn't come out until much later. "Jac" Casanova—great cryptologist.

In 1863, as I said, over a hundred years later, Major Friedrich Wilhelm Kasiski published in *Die Geheimschrift und die Chiffrierkunst* his method of factoring repetitions in periodic ciphers.

Then they come to codes. As you know, a code system is one using a

book containing letters, syllables, words, phrases, sentences, sometimes whole paragraphs. So that A-B-C-D-E in a 5-letter code might mean "I won't be back 'til Friday." One-part codes came into being early Renaissance.

Two-part codes... The first two-part code was by Rossignol, 1640, employed by Cardinal Richelieu. And there is a parenthetical side. Napolean's 200-group code was read by the Russians.

Now, early cryptanalysis. The first cryptanalyst was Daniel, 550 B.C. He read a cryptogram for Belshazzar. In Aramaic, it goes forwards, "mene, mene, tekel, (1G),": mean numbered, weighed and, of course, divided. Actually, (3-4G) has another cognate which is "feres," and "mene, tekel and "feres" are coins—money pieces. And accordance to Cyrus Gordon, this phrase actually means "You'll be quartered, halved, and sent to perdition."

In 1412, Qalqashandi—whom I mentioned before; the author of a 14-volume encyclopedia—gave the first exposition of cryptanalysis in history. He took word counts in the Koran and made statistics on native and (B% lone OR loan) words and also letter frequency data.

In 1474—actually Monday, July the 4th, 1474 for what that's worth—Cicco Simonetta wrote a little treatise on cryptanalysis—the first one entirely on cryptanalysis. He was secretary... This guy was in Naples and he was secretary to the first three Sforza dukes of Milano. He was executed in 1480.

1510, Giovanni Soro of Venice solved many ciphers including those of Charles V. Many ciphers intercepted by the Papal Court and not solved by it.

In 1525, England begins four centuries of successful cryptanalysis, marred only by the gap 1844 to 1914, which there's nothing doing over there politically speaking.

1556, (B% Matteo Argenti): he flourished under five popes. He had an uncle and brother as cryptanalysts. He was a very obliging cryptanalyst. He solved a message for the Portuguese ambassador who had lost his own cipher. This is of course ((audience laughs))... This is frowned upon today and... He lost his job in 1605, fifty years later, as a result of power play in the Papal Curia. It made me very happy to see that what is in NSA also happened centuries ago elsewhere. ((Audience chuckles.))

In 1567, the Great Vicar of Saint Peter's, according to Vigenère, quote, "deciphered in less than six hours a large page of cipher in the Turkish language ((he coughs)) (B% at) which he did not know even four words."

((Clears his throat and then takes a drink here.)) Prescription. ((Audience laughs.)) Water. ((More laughter.))
In 1589, François Viete—also known by his Latin name of "Vieta"—as Privy Counsellor to the King of France solved a 500-group code of Spain's Phillip II ((spoken as "the Second")). Phillip twitched—complained to the pope that France was using sorcery. So there was a miniature "Pearl Harbor" investigation on Viete, who, to avoid sorcery…conviction of sorcery—a capital offense—told all. In 1595, in June, the same Viete, by now a chronic blabbermouth ((audience laughs)), in conversation with the Venetian ambassador to France, revealed that his ciphers were being read. Tsk, tsk, tsk, tsk ((delivered somewhat facetiously)).

In 1626, Rossignol—remarkable for keeping his trap shut—began a cryptanalytic career with Louis XIII. When Louis was dying, he told the queen that Rossignol—of all things to say when you're on your deathbed…He told the queen that Rossignol was one of the most…one of the men most essential to the State. His 56 years as civil servant is equaled only by John Wallis. And Brigadier Tiltman is coming close to it.

In 1645, John Wallis—the greatest Englishman mathematician before Newton—began a career of five decades as an active cryptanalyst. He was under Cromwell—that is (B% cryptanalytically) speaking—and solves a secret cipher of Charles I. Brigadier Tiltman is now in his 46th year as an active cryptanalyst. 1689, Wallis solved the cipher of Louis XIV, which was a 600-group two- and three-digit code.

Now, let's skip to the Revolutionary War. In 1775, a…This makes a good story. A girl visited a baker—a girl with whom the baker had once been intimate. Visited him and asked his help in conveying a letter she had to the British. Well, he said he didn't want to do this, but he said, "Leave me the letter." And also, he wanted to get a double out because his own fiancé was about to appear on the scene. All this is authentic. I will not give you any business.

And, ah…But two weeks later, she wrote to him that, "You didn't do what you said you were going to do." But he opened the…He had opened the letter in the meantime and found some mysterious symbols. He showed it to a schoolmaster friend, who made nothing of it. When he got the letter from the girl, he went through channels to Washington—General Washington. And it seemed the letter was written by Dr. Benjamin Church, who was the Director General of Hospitals for Washington with whom the young lady was now, shall I say, more than she should be. There are youngsters in the audience and we have to temper the ((audience laughs))…But you are getting married? ((More laughter.)) When is this? Soon? Yes? ((Audience laughs.))

Well, Washington couldn't believe there was anything wrong—that is, as

far the communication is concerned. Alright! ((Chuckling heard.)) And he called in Dr. Church. And Church said that if deciphered, the letter would be perfectly simple—it's a letter to his brother. But Dr. Church didn't attempt to reveal what was in it.

So Washington gave the letter to two individuals: to Reverend Samuel West, and to Elbridge Gerry of "gerrymander" fame who later became 5th Vice President. And they were the first American cryptanalysts. They solved the letter independently. From the information from Church, General Gage captures the stores of Concord, which is the prelude to Lexington. Church was exiled to the West Indies, but the ship disappeared and nothing was ever heard of him again—which is a fitting tribute. He wasn't a traitor; he was just a sympathizer.

Then, of course, we have the case of Benedict Arnold and John André. Arnold used a book cipher—page, line, word: dictionary code—to which "7" was added—the digit seven. And also, a grill in the shape of an hour glass. In this period—the Revolutionary War—they would use secret inks and simple substitution sometimes with variants; the Vigenère Table with short (B% repeating) keys; and the pigpen cipher—Masonic cipher by various names.

James Lovell, a member of the Continental Congress, was actually the first cryptanalytic agency. He was a…sort of a one-man NSA. He read British simple substitutions—in those days we weren't buddies—and multi-alphabetic substitution in section. Every four lines…from four to ten lines were enciphered in one key and then shift. He used Vigenère system where A plain was "James"—happy thought—with John Gates. And with somebody else, he used "Cupid"—which was Madison's slave boy. Madison and Jefferson, Franklin used the systems, of course. Jefferson used two-part code. Franklin used a (B% French) sentence with the letters numbered, so he had variants for the high-frequency letters—was (B% their OR the) scheme.

Now we come to the Civil War. In 1861, the South was using simple substitution—Vigenère systems with word lengths preserved and words in the clear in the message. Jefferson Davis used a dictionary code where you had…The first number was the page; the second letter was the… L-M-R was left-hand, middle- or right-hand column. Then came the number of the word on that page. For instance, "146 L 20" stood for the word "junction" in their dictionary. Union intercepts were published in papers in Richmond and were advertised for solutions.

The North, on the other hand…And since we're…This is actually the gateway to the South, I suppose. But in any case, the North used word transposition including code words, indicators, and nulls. The North solved practically everything that came their way. I wouldn't have said this in a speech in Georgia. And the South, as I said, had difficulty getting

anybody to read anything.

Now, we come to cipher devices. In 1470, Alberti was the first inventor of the cipher disk. In 1500, there were a number of inventors that published ideas of disks.

In 1867, was the first significant breakthrough in a cipher device. Sir Charles Wheatstone, who had great interest in cryptology, invented a device which he modestly called "The Wheatstone Cryptograph." This was a geared gimmick which provided for a very irregular shift of the two sliding components. This is 1867. But like the Russians, we got there first—"we" on my wife's side. My wife is...Well, it's to my wife I owe my clearance. ((Audience chuckles.))

In 1817, fifty years before, this same device was invented, in fact, on a much better principle, and much better mechanical execution. It was invented by Decius Wadsworth who had been Chief of Ordnance, U.S Army. This is (B% like) 1812.

By the way, Wheatstone was also the inventor of the concertina and the inventor of the...He didn't invent the Wheatstone bridge. Let me give you the story straight. The Playfair cipher was invented by Sir Charles Wheatstone. Lord Lyon Playfair happened to be the sponsor of the British Foreign Office—and he gave it his name just in passing. So Wheatstone didn't get credit for the Playfair cipher, which he *did* invent. On the other hand, Wheatstone did get credit for the Wheatstone bridge, which he did *not* invent. See? ((Audience chuckles.)) So it balanced out. Actually, Wheatstone ((audience laughs))...Wheatstone applied Christie's...Samuel H. Christie's invention to the measurement of resistances.

In 1891, (B% Stevie) Bazeries...Étienne Bazeries wrote a book which was published actually in 1901. And he invented a system which...the Bazeries cylinder, the Bazeries cryptograph. A buddy of his, the Marquis d'Viares, in 1893, showed the general solution of this device. But this didn't faze Stevie, who still insisted this was the indecipherable cipher. The title of the Bazeries book was *Les Chiffres* (XG in French).

The same device was invented by a number of people later on. Parker Hitt in the U.S. Army made a flat version—a strip version of the device. But Jefferson, who was not only a great cryptologist but also a president, in papers discovered in (B% 1922) had the same idea of a device using 36 disks. And he gave the method of construction and of use of this system. The M-94, which is the U.S. version...the official version of this device, was used between 1923 and 1942.

Now we come to World War I. And thank God we don't hear this anymore. But a few years ago, every NSA speech began or had some place in it the phrase "Radio is a two-edged sword." Some idiot started it way back.

And then it's been perpetuated. So radio is a two-edged sword. ((Audience laughs.)) No.

The Battle of Tannenberg was the first big communications fiasco in history because, after all, World War I was the first time that the radio was used extensively. On the 26th of August was that famous battle. Rennenkampf, Commander of the First Russian Army, and Samsonov of the Second Russian Army. Rennenkampf got the new code and he promptly destroyed his old code. Samsonov was out in the field and didn't have the new code. Rennenkampf sent—who by the way didn't get along with Samsonov, not even on staff level—sent messages to Samsonov which he couldn't read. He was asked to relay the old code which Rennenkampf didn't have. So he gave his message in the clear.

The Germans couldn't believe their ears. They sent out patrols to scout out to see where...if the Russians *were* where they said they were. And they were. So everyday...It wasn't everyday for long; just three days. Every day the Germans waited for the day's...the morning's intercepts. And in three days, there are a hundred thousand ((100,000)) prisoners and 30,000 dead or missing.

On September 14, the German light cruiser *Magdeburg* was sunk in the Baltic. A Russian ship was nearby. And there are bodies floating ,and they wanted to give them a decent burial. So they picked up the bodies as they came along. And one chap was a (B% non-comm in rigor mortis). Actually not like this—you don't stand at attention when you're dead. ((Audience laughs.)) With the codebooks in his arms, locked. So they fished out the codebooks. Gave the guy a good burial and sent the code and signal books to the British. Actually, the naval attaché gave them personally to Winston Churchill. It's a wonderful find.

The Zimmermann telegram is perhaps the most famous cryptogram in history. On 16 January of 1917—we weren't in the war yet—Arthur Zimmermann, the Foreign Minister in Berlin, sent a telegram to Von Bernstorff in Washington—the ambassador to Washington—for transmittal to Von Eckardt, the ambassador in Mexico. Now, he was using our facilities, which is dirty pool.

Now, in this telegram, Mexico was being offered the lost territories in Texas, Arizona and New Mexico. And they wanted to get the Japanese on (B% the other) side and...if Mexico of course would declare war on the United States. We were having difficulty getting into the war. Wilson...Well, as a naturalized citizen, I don't want to criticize a former president, but see me later. ((Audience chuckles.)) Wilson was not the kind of a president that I would like to see heading our country and...However, this did it.

But when the British, who, by the way, were most reluctant to send us the

message because they had to reveal what they were doing. Finally they had a story leaked out to the press that this was intercepted...the plain language was captured in an American telegraph office. Anyway, the nation was shocked that the Germans were guilty of such complicity. And six weeks later we entered the war on the side of the Allies. If we hadn't entered then, who knows, it may have been an entirely different...Well, naturally, it would have been entirely different. It could have been very bad for England.

In this period...I told you that until 1914...from 1944 [sic] to 1914, there's no British Black Chamber. 1914: they were caught with their togas up. ((Audience laughs.)) And they started an activity called Room 40 OB. "OB" didn't stand for what you think it is or even "Order of Battle." Actually: "Old Building." ((Laughter heard.))

And Sir Alfred Ewing was the boss man. And immediately in charge of the project was Captain William Reginald Hall, a very brilliant cryptanalyst. When we—"we" on my wife's side—went to war...world war, the U.S. Army had three systems.

((1)) The cipher disk ((with)) reverse standard alphabets, which is a couple of centuries old. And you didn't need to read several messages—I mean, have several messages in depth. All messages could be put in depth. But you'd read one message in toto. Or read the first fifteen letters of any message because they used plain language keys. Well, that was the mainstay of our cryptography.

((2)) The War Department cryptography code which is sort of secure because (B% it's fat). Therefore, if it's under your blouse, you can see a bulge. Unless it's a tumor. I mean, it had to be something else. ((Audience laughs.))

((3)) And for the emergency system was the Playfair cipher. Are you getting most of the words, by the way? It's important to get a...It's alright to get a stream and then miss a stream. But don't get every other word because the continuity is very difficult. The Playfair cipher: which is known to be weak. In fact, every SOI which gave the keyword for the next two days—emergency keyword—would say, "Please try not to use it because it's weak. It's unsafe."

There are local unauthorized systems like codes made up: "Ty Cobb went to bat." Or "Red Grange..." Well, wrong period and wrong game, but anyway, you know: "Red Grange did something." And that meant "There's one tank coming over the hill."

There were two-letter and two-digit trench codes—one-part. The weakest of systems; and to which was sometimes applied a two-alphabet encipherment. Then came three-letter, two-part codes: the River series for the First Army, and Lake series for the Second Army. We learned from the Germans, and we became very proficient in printing and distributing

codes within two days. Other parties, the British included, took at least a week for the operation.

The Germans in World War I used double transposition, a rather complicated polyalphabetic cipher, and a system known as ADFGVX system. It used only those six letters. Originally it was only five letters. Only those six letters appeared in the cipher. And one strange thing about this system is that if you had a long message—let's say a 200-group message. And after sending 100 groups, there's a power failure on the part of the transmitter, you could reconstruct the entire message—the other side—not by guessing. We don't have any system like that today.

The Germans, in testing their systems, on the day of a change...key change would send a short axiom or parable, the most frequent of which was *"Morgan Stunde hat Golden Munde"*: The early bird catches the worm. So when the Allies caught wind of what was going on, on the day of a change, they searched through the early morning's traffic. Found a short message. Put the "early bird" against that. And by noon, they had the system.

We were in difficulties in corresponding with the British cryptographically because there wasn't a good...a secure system. The British knew what system...how weak our systems were. We didn't at the time.

Now, this Wheatstone cryptograph invented in 1680...by...in 1867 by Sir Charles ((Wheatstone)) was adjudged unsolvable if you had two unknown mixed components. The British knew how to solve the cipher if the plain component was a normal sequence or any other known sequence. So they decided they didn't want to use this device in World War I because the Briti...the Germans would capture this and they, too, would have an indecipherable cipher.

But we decided to cast caution to the winds with (2-3G), and introduce this for joint U.S.-British communications. The system was adjudged unsolvable in London and also at GHQ (B% AEF) and also in Washington. But somebody in Washington remembered that out in Geneva, Illinois there's an outfit called the Riverbank Laboratories, commercial laboratories. And there was in this...in these laboratories, a Department of Ciphers.

I want to backtrack a minute. The boss man was a Colonel George Fabyan. He really wasn't a colonel; it was an honorary thing for helping the peace mission. And Fabyan had an interest in Baconism. He wanted to prove Bacon wrote Shakespeare or vice versa or something. And he got a young lady in the...in his employ—a biologist by the name of Elizebeth Smith—to study up what there was in English—there weren't many books—to help him with his hobby.

Then in...In the same outfit, was a young geneticist, William F. Friedman, who was mating fruit flies—actually helping them to mate. ((Laughter from audience.)) And ah...Thank you. Friedman became a student in one of Miss Smith's classes. And he had a very fine aptitude, and he later took over the section. And a little bit later, he took over Miss Smith—she became his wife. ((Audience chuckles.))

Now, what happened was this, that the Br...There was sent from Washington six short messages to Riverbank in the vicinity of 30, 35 letters. Now, this is no test at all. Friedman knew how to solve...He discovered how to solve the classic Wheatstone, but didn't know what to do if you had two mixed sequences. However, by fiddling, he got out by a very strange process. I've read the solution, but I can't make head or tail out of it. He managed to get out the cipher component, which is a transposition mixed sequence based on cipher.

So he called in Miss Smith. She was still Miss Smith at the time. "Go sit down. Put on lipstick. Make yourself comfortable." He's going to give her a word—and "Please, give me the first one that comes to your mind." He said, "cipher," she said, "machine." Sure enough, the plain component was transmission signals based on machine. So the solution went back to the British—a very hazy account of how he got the cipher component. And as for the plain component, he asked Miss Smith. She gave it to him. ((Audience chuckles.)) So that was at Riverbank Laboratories.

In the early '20s, we have the advent of cipher machines. We began perhaps with Arvid Damm—D-A-M-M—who was quite a character, a brilliant inventor of weak systems. And he was a...He was a chap like you and me. I mean, a kind of a guy we like to know. He was evidently quite a...I guess "Lothario" is alright to say in mixed company. Well, quite a guy.

And he became enamored of an Hungarian circus rider—now I checked this with my wife last night and she says it's okay to say it—who said "Nothing doing" without a ring on her finger. Alright. ((Audience chuckles.)) And so...And he was in the heat, I suppose, of passion. And he got a buddy to dress up in priest's robes and marry them in a fake ceremony in a chapel in Finland. ((More laughter heard.))

Then, being quite a guy, he became enamored...You know, a series...Well, finally, there's one enamoration of his. Ah...(B% Sidney), what is the word? What's the gerund?

Sidney?: (XG; very faint.)

Callimahos: Well, whatever it is. ((Addressing Sidney:)) Thank you. You're helpful. ((Audience laughs.)) He became enamored on the train. Even on the train...You know, what else have you got to do? ((Audience laughs.)) Young girl in her twenties. And he was beside himself with joy. So he decided to divorce his wife. But actually he hadn't even been married, and

his divorce proceedings weren't legal either. So to make sure that it took, he accused his wife, in quotation marks, of being "a spy." But he was betrayed by a very famous cryptologist, (B% Eve) ((Olof)) Gyldén, who got his comeuppance because when Damm reorganized the company, he did not give the general manageship to Gyldén. So there.

Then he went with his fiancée to—I guess it's alright: fiancée—to Paris where they stayed together, for what that's worth, at the Hotel (B% Perigor), in case anybody... I don't think it's still standing today. But that's where they went. ((Audience laughs.)) After... Look, it's always good to file and forget, you know, information. The Hotel Perigor. But when he turned over his villa to her, he got his comeuppance because she jilted him for somebody else. These are real people. ((Audience laughs.))

Okay. Now, he invented a number of devices. This firm, which didn't do well financially, was taken over by one of his young engineers—a chap by the name of Boris Caesar Wilhelm Hagelin.

There are other firms. There's a firm started by a chap in 1924: Alexander von Kryha, who invented a remarkable device or so he thought, with a fantastic number of possibilities. He got a buddy mathematician to write a mathematical exposition as to the security. And you could never solve it in... you know, in a zillion years. Ah, he calculated... The mathematician calculated that the parameters of the device were 1.4 times ten to the 64^{th}. Actually, for practical purposes, you can ignore the coefficient. Ten to the 64^{th}. And since the number of atoms in the universe is ten to the 74^{th}—I didn't count them; it's Sir Char... Sir Arthur Eddington—you'll see it compares very favorably.

Now, in the late '20s, Boris Caesar Wilhelm Hagelin marketed several devices: the B-21, B-22, B-211 in the late '20s. These are fractioning devices with rather long periods. Then he made a series of devices: the C-36—the numbers stand for the years—C-38, etcetera. The C-38 has a period of 101 million letters. It's the M-209 in our own service. This actually is Vigenère substitution with six simultaneous simple substitutions that are in or out.

Well, I see time is a-wasting, and we have seven minutes. So I'll do some skipping.

In 1923, Sir Edward Hebern invented what he modestly called the Hebern Electric Super Code. It was a one-rotor device. Then he went from that to a five-rotor machine. Then he went back to a one-rotor device. Then he sold (B% a KKK). He knew what he was doing. ((Audience chuckles.)) Now, this machine had a potential with five rotors. They could put forwards or backwards, right side up or upside down five rotors; and the

current going either left to right or right to left. Had a potential of 90 billion (B% cipher) alphabets.

This young cryptanalyst, William Friedman, who by now was a temporary civil servant with the Signal Corps—he was temporary for about 35 years—solved the device on ten messages submitted by the Navy. The Navy was interested. He'd...The Navy had bought some copies and had promised Hebern a big contract. But Friedman solved them on ten messages. Actually, he did what a mathematician wouldn't have done because the cards were against him. But Friedman was abysmally ignorant of mathematics. In fact, Friedman was cursed by luck throughout his entire career. ((Audience laughs.)) Yeah. It seems everything he touched turned to plaintext. ((More laughter.)) Yeah. With exception...with the exception of Miss Smith. No. ((More laughter.))

Friedman, whenever he wrote a mathematical (B% solution), he was invariably wrong. He made colossal errors. But I'd say, it still...Because he made so many errors, one of his errors had to be on the right track. ((Audience laughs.)) So he solved this machine. The Navy wrote back to Hebern. Hebern revised the machine. Friedman solved them again. And the Navy didn't...cancelled the contract. Then Hebern did something wrong with the California stock laws and he went to jail. And he was much teed off. And then after the war...After the war's end, he sued the Government for 50 million dollars. And then his estate continued the suit. And finally, he got some small token. I don't want to get involved in that controversy.

But on large numbers, I might point out that I invented a machine. I've invented a number of very weak systems. Any guy can invent a good system, but it takes brains to invent good weak systems. ((Laughter heard.)) No. These...No. These were used by the maneuver enemy on joint maneuvers and training exercises in the U.S. Machines and code systems and other manual ciphers. And this one machine makes a furious clatter; painted (B% violent) green; has for the number of parameters 10 times 10 to the...3 times 10 to the 82nd different changes. And our best U.S. equipments at that time had only 10 to the 41st parameters. This number that I gave you is one hundred million times bigger than the number of atoms in the universe.

Now, in...We come briefly to teletype systems. In 1917, a young engineer, Gilbert S. Vernam, showed to Signal Corps authorities an idea of a one-tape...of a keying tape to key a message tape. Well, the Signal Corps didn't like that and Vernam proposed a two-tape system. And this was...The weakness of this was shown early by Friedman and company.

Then came a...an...a machine marketed, devised by the ITT. It took four years to make a quarter million dollars. That had a large number of changes—almost 10 to the 15th. And this was solved by Friedman and company in about three hours. ((Audience chuckles.)) I have to skip the bit on ciphex and ciphony. Gee!

World War II. In World War II, COMINT success...And this...By the way, all this is unclassified. All this...But this is coming from *Time* magazine of December 1945. COMINT successes in...during World War II enabled a relatively small U.S. force to intercept the Japanese invasion fleet and win a decisive victory in the Battle of the Coral Sea ,thus saving Australia and New Zealand. It gave the U.S. full information on the size of the Japanese forces advancing on Midway. Enabled the vict...the Navy to concentrate the ships which otherwise might have been 3,000 miles away—and thus set up an ambush which proved to be the turning point victory of the Pacific war.

It directed U.S. submarines unerringly to the sea lanes where Japanese convoys would be passing. And made possible the reading of messages from the Japanese Ambassador Oshima in Berlin—often reporting interviews with Hitler, giving our forces invaluable information on German war plans.

I might point out that there's a glorious write-up of our common effort in the Report of the Joint Committee, Pearl Harbor Attack. And I'll just give you a brief quote: "The success achieved in reading the Japanese diplomatic codes merits the highest commendation. And all witnesses familiar with MAGIC material"—MAGIC was the codename at the time for this type of intelligence—"throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

General Chamberlain, MacArthur's G3 in the Pacific, said that it shortened the war by no less than two years. And that time it was estimated that one dollar spent on COMINT was equivalent to one thousand dollars spent on other (B% works).

In...On 18 April 1943, Admiral Yamamoto, Chief...Commander in Chief of the Combined Fleet, Japanese Forces, Japanese Navy, was shot down in the Solomons ((Islands)). Why? We had read a message five days before, giving his itinerary. Of course, the information had to be disguised...The picture had to be disguised so that it was "reconnaissance planes which spotted him".

: I have about one (1-2G) left. Cryptology since World War II.

Actually, the Navy effort was our...the first one...first official effort in our country. OP-20-G, the Navy cryptologic effort, started in 1924. SIS, the Signal Intelligence Service, in the Army, in 1929. The AFSS, the Air Force counterpart, started in 1948 after the Air Force became a separate entity.

AFSA started in July 1949. And since things weren't going too well as this joint agency, it was changed to NSA in November of 1952.

Our growth of cryptologic effort has been tremendous. In World War I, there are only 400 people in COMINT. It's 1 to 10,000 under arms. In World War II, we had 16,000 people—forty times greater: 1 in 800 people.

What characterizes our present day—at the unclassified level—our present day effort is the fact that we...that technology has advanced to such great degrees. Mechanization of problems and conceptions of cryptanalytic attack that simply were impossible sometimes even as far...as little as five years ago.

Before World War II, cryptanalysis was really very infantile. There were tremendous advances. There's an exponential curve in World War II. Cryptology made astonishing advances. And after that, there's been, you could say, as great a growth after World War II as there has been during the war years.

Now, there's no time for questions. But if you have any questions of an unpersonal nature, I'll be glad to answer them. Well, isn't anybody going to do anything? ((Mr. Callimahos claps. Then the audience laughs and follows suit—they begin to applaud also.)) ((TR NOTE: Audio abruptly ends at this point.))

//**End of transcript**//